DORAM: What is? Why Care? What Did we Do?

Maliciously-secure DORAM with the best-known semi-honest asymptotics.
Fastest DORAM for large (proj: $> 2^{21}$)

Brett Falk[1], Daniel Noble[1], Rafail Ostrovsky[2], **Matan Shtepel[2], Jacob Zhang[23]**

[1]University of Pennsylvania

[2]University of California, Los Angeles

[3]Jane Street

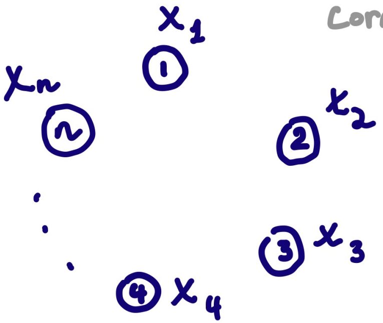
January 12, 2023

Overview

1. Preliminaries
2. DORAM Uses
3. Our Contributions
4. Future Work

Prelemenaries: What is Secure Multi-Party Computation (MPC)?

$f \in PPT$



everyone wants:

Correctness →

- $f(x_1, \dots, x_n)$
- not reveal x_i

↑ privacy

Prelemenaries: Semi-Honest vs Malicious Security in MPC

Semi-Honest security: if everyone follows the protocol precisely, security is gurenteed.

Malicous Security: no matter what anyone does, security is gurenteed.

Prelemenaries: What is ORAM?

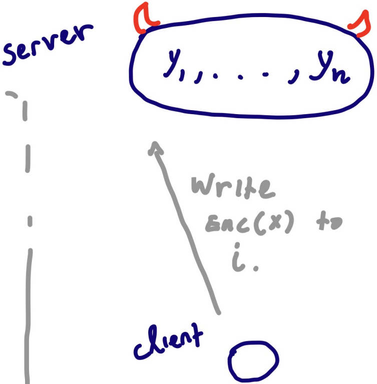
classic paradigm:

- lightweight client stores Enc(data) on Server

Problem:

leaks Access pattern

Sol: Oblivious RAM



Prelemenaries: Bottlenecks of ORAM

- $O(\log N)$ interactive sequencial rds per r/w query
- Each ORAM serves a single client
- Complex client
- Amortized (bad phases)

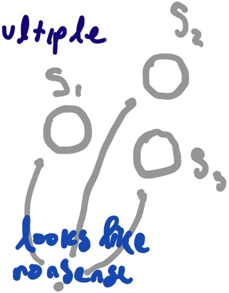
(we simplify here, there have been works attacking this, largely still issue)

Prelemenaries: What is DORAM?

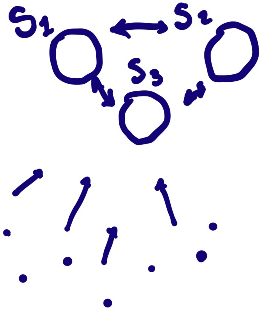
Distributed Oblivious RAM is a Relaxation of the problem.

<u>Add</u>: trust assumption, multiple servers, Some are honest.

<u>Ask</u>: Can we do better?



DORAM Uses: ORAM-replacement supporting many extremely-lightweight clients



! Why care? !

- lots of clients!
  ↳ extremely simple
  — no install needed
- 3x overhead over trusting client

instead of $O(\log N)$ Amortized

- 1 rd per query

(instead of $O(\log N)$)

DORAM Uses: MPC in the random access model RAM-MPC

circuits are a pain!

why care?

+ circuits are less efficient

DORAM enables RAM-MPC

(write python‡ instead of circom)

Our Contributions: Theoretical Contributions

Let N be the number of elements stored in the DORAM, D be the payload size, κ be the computational security parameter.

Theorem (DORAM, informal)

There exists a (3,1)-MPC maliciously secure MPC scheme on bits or fields with $O(|C|)$ *communication and computation complexity which achieves* $O((\kappa + D)\log N)$ *amortized communication complexity and amortized computation complexity per random access.*

only semi-honest was known.

Theorem (RAM-MPC, Informal)

There exists a (3,1)-DORAM scheme which achieves $3(\log N + D)$ *client query communication complexity,* $O((\kappa + D)\log N)$ *amortized* $\{$*communication,computation*$\}$ *complexity between the servers per query, and* **non-amortized** *1 round of interaction per query for client.*

only semi-honest was known.

Our Contributions: Practical Comparison with Existing DORAM

Takeaway (mostly projected): for practical databse sizes and good networks, we improve on previous and concurrent semi-honest works by a factor of 10x-100x. [1]

Expect benchmarks on Saturday, but roughly, at $N = 2^{20}$ we able to get while state of the art can do 600 queries (semi-honest) while state of the art can do 1 query per second (semi-honest)

[1] our tests are not precise (yet)!

Our Contributions: Open Source EMP-Toolkit code

EMP Toolkit (158 GitHub stars) – we're workin on it!

Thanks Everyone!

Demo! (with DORAM chant)

goto https://matanshtepel.com/DORAM/HackLodge_demo.html